檔　　號:
保存年限:

臺中市政府教育局 函

地址：411臺中市太平區樹德一街136巷30號(資網中心)
承辦人：課程督學 陳淑珍
電話：23952340#112
電子信箱：chcsj@taichung.gov.tw

受文者：臺中市梧棲區梧棲國民小學

發文日期：中華民國109年12月30日
發文字號：中市教資字第1090112699號
速別：普通件
密等及解密條件或保密期限：
附件：附件1臺中市政府來文、附件2行政院來文、附件3各機關資通安全事件通報及應變處理作業程序（387040000E_1090112699_ATTACH1.pdf、387040000E_1090112699_ATTACH2.pdf、387040000E_1090112699_ATTACH3.pdf）

主旨：函轉行政院訂定「各機關資通安全事件通報及應變處理作業程序」乙份，請各校(園)據此修訂資通安全推動組織並納入110年資通安全維護計畫後留校備查，以利完成資安事件通報、應變、損害控管及跡證保存等作業，請查照。

說明：

一、依據本府109年12月1日府授資網字第1090295435號函辦理。

二、本案係本府函轉行政院訂定「各機關資通安全事件通報及應 變處理作業程序」(附件3，以下簡稱本程序)，自即日起 生效，試行一年案，期滿由行政院資通安全處瞭解執行狀況，俾供後續檢討評估。

三、有關本程序重點摘要說明如下：

(一)本程序主要為提供各納管公務機關預先參照各分組代表建 議人選，建立校（園）內通報及應變小組各分組代

教務處　　收文:109/12/31
1090005950　　有附件

表，以利資安事件發生時，迅速成立通報及應變分組，依法遵時限完成通報、應變、損害控管及跡證保存等作業，先予敘明。

(二)各校（園）可參照本程序第二點第二項「各機關得以現有分組為基礎，依各機關編制及業務分工，經機關資通安全長同意後調整通報應變小組組成及各分組代表」之說明調整貴機關資通安全維護計畫第伍章「資通安全推動組織」，並可視機關資安責任等級及組織編制，整併組別及成員，惟仍須經機關資通安全長同意，若有修正資安推動小組組織請納入110年資通安全維護計畫，並經逐級核章後留校備查。

(三)為確保資安事件不再重複發生，因此每次資安事件均需調 查其根因作為改善基礎，並依規定保存相關跡證，如發現惡意程式，應上傳至Virus Check網站(https://viruscheck.tw/)進行檢測；因故無法上傳時，應送交防毒軟體或資安服務公司檢測。

(四)依據事件調查報告，各校（園）應評估短、中、長期資安管理改善策略，其內容如下：

1、短期：完成可立即性修補項目之調整，例如更換密碼或修補程式弱點等。

2、中期：依據事件根因提出三至六個月內完成之強化作為，例如盤點機關老舊設備，並訂定汰換期程。

3、長期：依據事件受害情形，視需要提出二年內完成之管理改善建議，例如培養機關資安人員能力。

(五)對於調查過程所需之日誌應事先規畫於平日即妥善儲

存，發生資通安全事件時，機關應依下列原則進行跡證保存：

1、機關進行跡證保存時，應優先採取隔離機制，包含設備 關機、網路連線中斷或隔離、關閉服務、限制連線、限 制權限、有限度修補漏洞等方式，以降低攻擊擴散。

2、若系統無備援機制，應備份受害系統儲存媒介(例如硬 碟、虛擬機映像檔)後，以乾淨儲存媒介重建系統，於完成系統測試後提供服務。

3、各校（園）於簽訂資通系統或服務之委外契約時，應依前二款規定於契約中定明紀錄保存及備份規定。

四、本府原函頒「臺中市政府暨所屬機關資通安全事件通報及應變管理程序」，自即日起配合旨揭作業程序同步廢止。

五、邇後本局將函請重複發生資安事件之學校（及幼兒園），提供事件根因調查報告及改善策略，以降低資安事件重複發生之比率。

正本：臺中市各市立高級中等學校、臺中市各市立國民中小學、臺中市各市立幼兒園（不含和平區）、臺中市和平區幼兒園
副本：本局課程教學科、本局資訊教育暨網路中心 電子公文交換章 2020/12/31 13:32:48